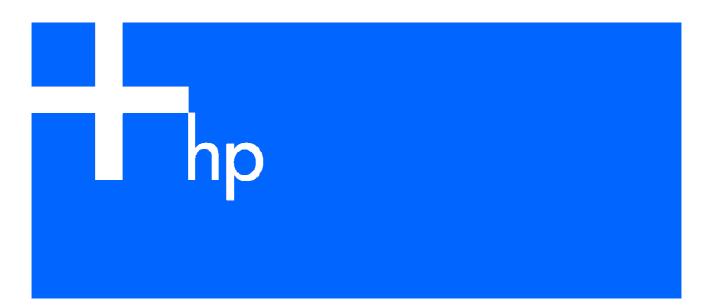
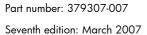
HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix







Legal notices

© Copyright 2004–2007 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. Windows Server 2003 is a U.S. trademark of Microsoft Corporation. Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

Part number: 379307-007 Seventh edition: March 2007

Contents

А	bou	t t	hı	IS	a	UΙ	d	е

Where to go for additional help	4
HP contact information	4

Vulnerability and Patch Management Pack

HP Systems Insight Manager

VPM Acquisition Utility (optional)

Target systems

Supported applications

About this guide

This support matrix lists requirements for all components in an HP ProLiant Essentials Vulnerability and Patch Management (VPM) Pack environment. Supported target systems and applications are also included.

Where to go for additional help

In addition to this guide, the following information sources are available.

For additional information about Vulnerability and Patch Management Pack, see:

- http://www.hp.com/go/vpm
- HP ProLiant Essentials Vulnerability and Patch Management Pack Installation Instructions
- HP ProLiant Essentials Vulnerability and Patch Management User Guide

For additional information about HP Systems Insight Manager (HP SIM), see:

- http://www.hp.com/qo/hpsim
- HP SIM User Guide
- HP Systems Insight Manager Help Guide

HP contact information

For the name of the nearest HP authorized reseller:

- In the United States, see http://www.hp.com/service locator.
- In other locations, see http://www.hp.com.

For HP technical support:

- In North America:
 - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week.
 For continuous quality improvement, calls may be recorded or monitored.
 - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, see the HP website http://www.hp.com.
- Outside North America, call the nearest HP Technical Support Phone Center. For telephone numbers for worldwide Technical Support Centers, see the HP website http://www.hp.com.

Vulnerability and Patch Management Pack

The VPM server, the server on which Vulnerability and Patch Management Pack software is installed, must meet the following hardware and software requirements. Requirements listed for the VPM server are independent of requirements for HP SIM and any other applications that coexist on the VPM server. For specific hardware and software requirements for the HP SIM server, see the HP SIM User Guide.

Table 1 Hardware requirements

Component	Specification	
Any HP x86 server —		
Memory	At least 512 MB RAM	
Processor	1.5 GHz or higher	
Disk space	1 GB for Vulnerability and Patch Management Pack (150 MB in the TEMP directory for installation)	
	Additional space for scan reports and patches	
File structure	New Technology File System (NTFS)	
DVD-ROM drive	_	

Table 2 Software requirements

Component	Specification	
	Microsoft® Windows® 2000 Server SP4	
Operating system	Windows 2000 Advanced Server SP4	
(32-bit versions	Microsoft Windows Server™ 2003, Standard Edition SP1	
only)*	Windows Server 2003, Enterprise Edition SP1	
	Windows XP Professional SP2	
Services	Microsoft Internet Information Services (IIS) 5.0 or later, installed and running**	
Jervices	TCP/IP with DNS properly configured so that system names can be resolved to IP addresses	
Database	An existing Microsoft SQL Server database can be used, or Microsoft Data Engine (MSDE) will be installed on the VPM server with the Vulnerability and Patch Management Pack installation. When changing databases during an upgrade, patch data from the previous database is not migrated. A ful patch acquisition must be performed to repopulate the patch repository.	
Applications (must be available on the network)	HP SIM 5.1 or later, installed and running on a Windows server with Windows Management Instrumentation (WMI) Mapper	
	Mozilla Firefox 2.0 or Microsoft Internet Explorer 6.0 or 7.0	
	Adobe® Acrobat® Reader 3.x or later (to view scan results)	

 $^{^{}st}$ HP SIM might have additional restrictions for supported service pack levels.

^{**} HP strongly recommends enabling HTTPS if HP SIM and Vulnerability and Patch Management Pack are installed on separate servers. For information about configuring HTTPS service in IIS, see http://support.microsoft.com/?kbid=324069.

HP Systems Insight Manager

HP SIM 5.1 or later must be installed on a Windows server. This release of Vulnerability and Patch Management Pack does not support HP SIM installed with a Linux or HP-UX operating system.

VPM Acquisition Utility (optional)

The VPM Acquisition Utility can be installed on a system with Internet access, enabling patch acquisitions and vulnerability updates without requiring the VPM server to be directly connected to the Internet.

Table 3 lists the minimum requirement for the system on which the optional VPM Acquisition Utility is installed.

Table 3 VPM Acquisition Utility requirements

Specification	
256 MB RAM	
1.5 GHz or higher	
12 MB	
Available space for downloading vulnerability patches	
Internet access (for downloading vulnerability patches)	
Windows 2000 Server SP4	
Windows 2000 Advanced Server SP4	
Windows 2000 Professional Windows Saver 2003 Standard Edition SP1	
Windows Server 2003, Standard Edition SP1	
Windows Server 2003, Enterprise Edition SP1	
Windows XP Professional SP2	

Target systems

Target systems are managed by Vulnerability and Patch Management Pack. HP recommends installing HP Management Agents on ProLiant target systems to enable HP SIM to better identify the target systems. Enable WMI or Web Based Enterprise Management (WBEM) for other target systems. The VPM Patch Agent is automatically deployed when target systems are licensed to enable patches to be applied to the systems.

Secure Shell (SSH) must be installed on Linux target systems.

Table 4 lists the 32-bit operating systems that Vulnerability and Patch Management Pack supports.

 Table 4
 Target operating systems

Component	Specification	
	Windows 2000 Server SP3 or later	
	Windows 2000 Advanced Server SP3 or later	
	Windows 2000 Professional SP3 or later	
	Windows Server 2003, Standard Edition	
	Windows Server 2003, Enterprise Edition	
	Windows Server 2003, Web Edition	
	Windows Small Business Server 2000	
Operating system (32-bit versions only)	Windows Small Business Server 2003	
,	Windows XP Professional	
	Red Hat Enterprise Linux 2.1 ES for x86*	
	Red Hat Enterprise Linux 3 ES for x86*	
	Red Hat Enterprise Linux 4 ES for x86*	
	Red Hat Enterprise Linux 2.1 AS for x86*	
	Red Hat Enterprise Linux 3 AS for x86*	
	Red Hat Enterprise Linux 4 AS for x86*	

^{*} Red Hat systems must have a valid subscription to the Red Hat Network for patch acquisitions. A valid Red Hat Network license is required for each system to be patched. For information about subscribing to the Red Hat Network, see http://www.redhat.com.

The Red Hat library, compat-libstdc++, must exist on the Red Hat target systems.



NOTE: Vulnerability and Patch Management Pack is available in English (U.S.) for use only on English, French, Italian, German, Spanish, and Japanese versions of the operating system.

Supported applications

Vulnerability and Patch Management Pack supports patching of the following applications on monitored systems:

- All Microsoft applications for which patches are available (excluding Microsoft Office applications)
- All applications included with Red Hat Linux